10 ZASAD SKUTECZNEGO SECURITY AWARENESS

POZNAJ NAJWAŻNIEJSZE ZASADY I PODNIEŚ POZIOM CYBERBEZPIECZEŃSTWA

SecurityInside

LOGICALTRUST

00

WSTĘP

Cyberprzestępcy bezlitośnie wykorzystują nieświadomych pracowników, wykradają informacje i paraliżują działanie firm. Żądają okupu za odzyskanie danych, przy okazji grożąc opublikowaniem cennych dokumentów w sieci.

Skuteczna i systematyczna edukacja, trening i zwiększanie świadomości, mogą pomóc ograniczyć straty finansowe związane z incydentami bezpieczeństwa.

CEL

Po 16 latach wykonywania testów bezpieczeństwa i edukowania pracowników, wiem, że przygotowanie skutecznego programu Security Awareness nie jest łatwym zadaniem.

Mam nadzieję, że poniższy mini poradnik pomoże podnieść poziom kultury bezpieczeństwa w Twojej organizacji.

Borys Łącki
Security Ninja
LogicalTrust.net

01

BEZPIECZEŃSTWO = NUDA

> *Pracownicy mają bezpieczeństwo w (...) polityce bezpieczeństwa.*

Pracownicy działów bezpieczeństwa są często pasjonatami i myślą, że wszyscy powinni być zainteresowani *cybersecurity* co najmniej tak jak oni. Niestety takie myślenie powoduje, że słabiej docierają do koleżanek i kolegów.

Uważaj na własne *ego* - często naszym zadaniem jest wykazywanie niedociągnięć innych ludzi w edukacji, w temacie bezpieczeństwa.

Pamiętajmy, że **naszą rolą jest pomaganie, a nie tylko wytykanie błędów.** To drugie powoduje obniżenie motywacji pracowników do zaangażowania się w bezpieczeństwo.

Pracownik nie jest zainteresowany bezpieczeństwem, to nie jest jego główny obowiązek. To, że dla nas jest to bardzo istotne, nie oznacza, że dla naszych współpracowników jest tak samo.

02

WYBIERZ ESENCJĘ

Przeprowadź modelowanie zagrożeń dla Twojej firmy. Zastanów się co jest największym niebezpieczeństwem i edukuj tylko o najważniejszych aspektach.

Bezpieczeństwo to ponad setka różnych obszarów, m.in.: bezpieczeństwo fizyczne, chmura, świadomość pracowników, phishing itd. Pracownicy działu bezpieczeństwa chcieliby nauczyć współpracowników wszystkiego o bezpieczeństwie - to błąd.

Nie przytłaczaj współpracowników tysiącami zagadnień i skup się na kluczowych i aktualnych zagrożeniach.

Czy przy ograniczonej uwadze pracowników, warto dziś opowiadać o możliwych atakach przez fax? Czy może lepiej skupić się na złośliwych załącznikach, z którymi mamy dziś bardzo często do czynienia.

Pamiętaj, by ocenić, które ryzyka w firmie są największe i od nich zacznij edukację.

03

USZCZĘŚLIW MÓZG

Suche fakty nie działają. To historie są najlepszym sposobem na skuteczne przekazywanie informacji - tak działa mózg.

Jeśli w edukacji budujesz narrację w oparciu o techniczne detale, mózg szybko przestaje przyswajać informacje.

ŹLE: W wyniku braku aktualizacji na podatność CVE-2020-0901, złośliwe oprogramowanie wykorzystało błąd przepełnienia bufora, co umożliwiło eskalację do poziomu użytkownika o najwyższych systemowych uprawnieniach i skutkowało utratą dostępności w kluczowym obszarze zasobów serwerowych.

DOBRZE: Spotkałem przedwczoraj koleżankę z firmy, która ma biuro dwa piętra nad nami. Jeden z pracowników kliknął w załącznik z wirusem i cyberprzestępcy przejęli ich komputery. Dział IT wciąż próbuje odzyskać wykradzione dane, stracili już kilkaset tysięcy złotych i byli zmuszeni zwolnić trzy osoby.

04

DOPASUJ KOMUNIKAT

Organizacje i ludzie są różni. Pamiętaj o tym.

Wykorzystuj metody dopasowane do Twojej firmy i współpracowników.

Stosuj zasadę od ogółu do szczegółu.

Inne historie opowiadaj administratorom, inne pracownikom biurowym.

Pamiętaj, że strach działa demotywująco. Nie wytykaj błędów konkretnym osobom, lepiej pokaż, że istnieje ogólny problem w organizacji.

Starajcie się grać do jednej bramki i razem z koleżankami i kolegami zbudujcie efektywny human firewall.

05

DLACZEGO?

Pamiętaj by tłumaczyć dlaczego coś należy robić.

ŹLE: Należy stosować się do zasad związanych z bezpieczeństwem haseł. Polityka bezpieczeństwa określa, że hasło powinno składać się z minimum 12 znaków, 2 wielkich liter, 4 znaków specjalnych i 1 cyfry.

DOBRZE: Wytłumacz pracownikowi dlaczego ma korzystać ze skomplikowanych haseł, np. opowiedz o tym, że jeżeli nie będzie używał silnych haseł, cyberprzestępcy mogą wykraść dane z firmy, firma straci pieniądze i będzie zmuszona ograniczyć premie.

Badania pokazują, że rozumiejąc dlaczego coś mamy zrobić, działamy bardziej efektywnie.

06

SZANUJ CZAS PRACOWNIKA

Edukacja dziś to walka o uwagę człowieka. Jeśli chcesz by pracownik poświęcał godzinę tygodniowo na tematykę bezpieczeństwa (która go nie interesuje), skuteczność edukacji będzie bardzo niska.

Ważniejsza jest jakość, a nie ilość. Na naszej platformie e-learningowej każda lekcja trwa kilka minut i zawiera przyjemny w odbiorze film. Tylko krótka i ciekawa forma sprawi, że edukacja nie będzie odbierana jako coś nieprzyjemnego.

Pamiętaj by obniżać próg bólu koleżanek i kolegów, a będą chętniej wracali do zagadnień związanych z bezpieczeństwem.

07

KORZYŚĆ OSOBISTA

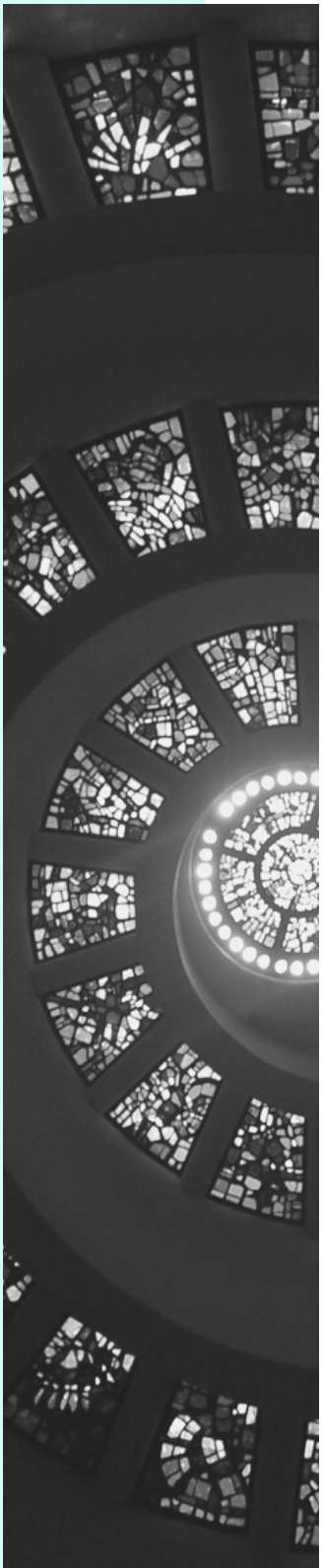
"Masz tak robić bo to jest ważne" - nie działa. Skuteczniejsze jest podkreślenie korzyści osobistej.

Na pracownika słabo działa straszenie, że firma straci ważne dla niej dane. **Do edukacji warto dodać kontekst osobisty.** Pracownik może stracić swoje prywatne dane np. zdjęcia z wakacji lub pieniądze z konta bankowego. W ten sposób nauczymy pracownika dobrych praktyk, które będzie przenosił do firmy.

Korzyść osobista może być szeroko rozumiana. Może to być ochrona wrażliwych danych i pieniędzy, ale dla niektórych cenniejsze mogą być np. rozwijane latami postaci w grach :) Ważne jest dotarcie do serc ludzi, zrozumienie ich potrzeb.

08

DZIAŁAJ PROCESOWO I SYSTEMATYCZNIE



Zaplanuj swoje działania na co najmniej rok do przodu.

Przeanalizuj swój budżet, zastanów się jak go optymalnie wydać. Pomyśl co możesz zrobić wewnętrznymi zasobami, gdzie warto skorzystać z darmowych materiałów, a w których działaniach wesprzeć się firmą zewnętrzną.

Działaj systematycznie ale nie za często. Setny e-mail ostrzegający o niebezpiecznych wiadomościach będzie bezskuteczny. **Działaj rzadziej ale ciekawiej.**

Newsletter warto rozsyłać w ten sam dzień tygodnia o tej samej porze, ale już testy socjotechniczne wykonuj o różnych porach.

Przynajmniej raz na rok zadbaj o wykład w przystępnej formie i wykonaj testy socjotechniczne. Efekt "wow" zostanie w głowach pracowników przez kilka tygodni.

Dostęp do platformy e-learningowej pracownik powinien mieć przez cały rok, by swobodnie z niej korzystać.

09

PROSTO I PRAKTYCZNIE

Porady powinny być zrozumiałe i użyteczne.

Tylko łatwe do zapamiętania i wygodne w użyciu rozwiązania, są w stanie sprawić, że pracownicy będą z nich korzystać.

Jeśli chcesz aby pracownik używał różnych i skomplikowanych haseł, to podpowiedz mu jak może łatwo zapamiętać skomplikowane hasła i naucz go korzystania z menadżera haseł.

10

ATRAKCYJNA FORMA

> *Jeden obraz wart jest więcej niż tysiąc słów.*

Pamiętaj o tym, że atrakcyjna forma jest w stanie zawładnąć uwagą pracownika na kilka minut. Świat zwariował na punkcie krótkich filmów, dlaczego nie wykorzystać ich w zwiększaniu świadomości? Ciekawy obraz statyczny lub ruchomy jest skuteczniejszy od treści pisanej.

Zadbaj o różnorodność treści i zainwestuj w różne strategie dotarcia do pracowników.

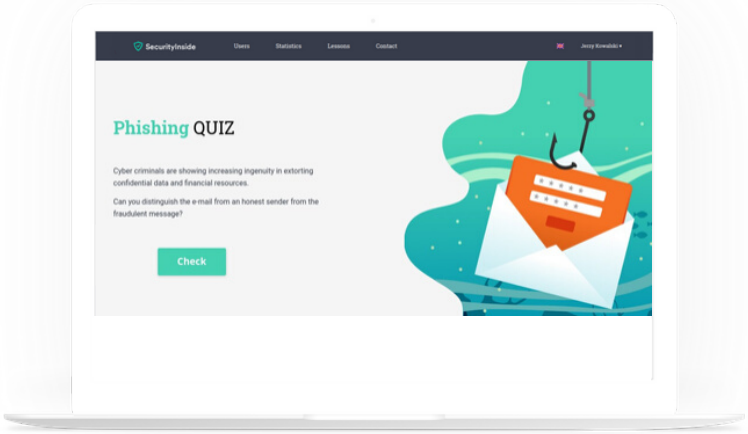
Drukowane plakaty, newslettery przesyłane e-mailem, grafiki, filmy, e-learning, ciekawe gadżety, testy socjotechniczne, wykłady na żywo. Każdy dobrze dobrany kanał komunikacji zwiększa skuteczność edukacji.

Pomyśl niesztampowo. Może zamiast dziesiątek standardowych maili z numerem telefonu do działu bezpieczeństwa (których nikt nie czyta), warto wydrukować ciekawą grafikę i umieścić ją w stosownym miejscu.

PODSUMOWANIE

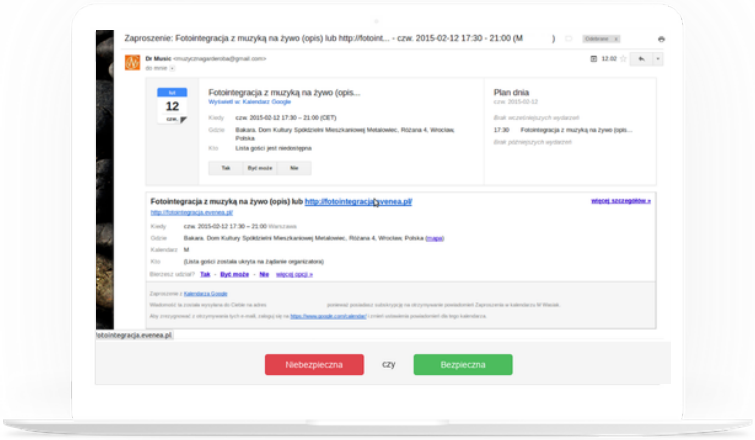
1. Bezpieczeństwo nie jest najważniejsze.
2. Edukuj o kluczowych zagadnieniach.
3. Używaj historii, a nie suchych faktów.
4. Dopasuj formę i treść komunikatu.
5. Wytłumacz dlaczego?
6. Jakość, a nie ilość, krócej znaczy lepiej.
7. Podkreśl korzyść osobistą.
8. Działaj procesowo i systematycznie.
9. Porady powinny być proste i użyteczne.
10. Zadbaj o różnorodną i atrakcyjną formę.

DARMOWE MATERIAŁY



https://quiz.securityinside.com/

Can you distinguish the e-mail from an honest sender from the fraudulent message?

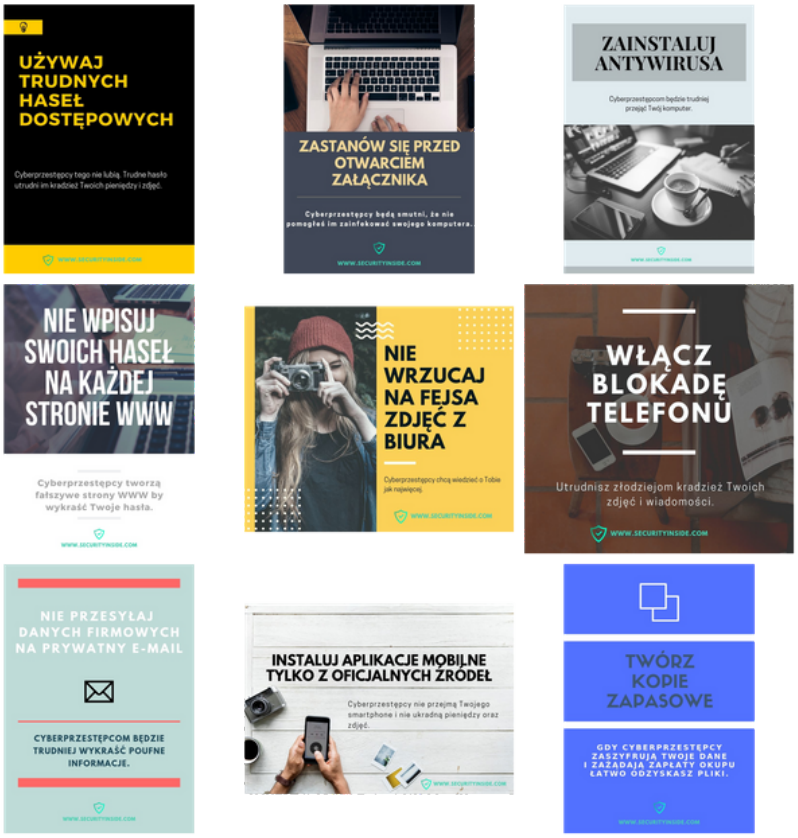


https://quiz.securityinside.pl/

Czy potrafisz odróżnić e-mail nadesłany przez uczciwego nadawcę od spreparowanej przez oszustów wiadomości?

DARMOWE MATERIAŁY

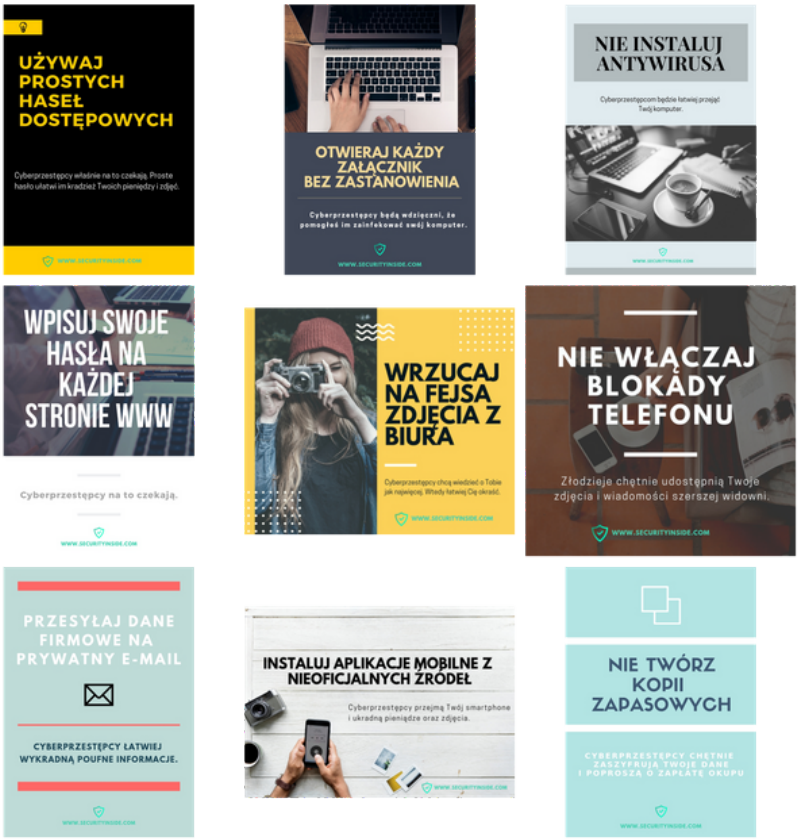
Plakaty - kampania "normal"



https://securityinside.com/free/files/securityinside.com-infographics-201907-pl-jpg.zip - PL

DARMOWE MATERIAŁY

Plakaty - kampania "rebel"



https://securityinside.com/free/files/securityinside.com-infographics-201903-pl-jpg.zip - PL

https://securityinside.com/free/files/securityinside.com-infographics-201903-en-jpg.zip - EN

DARMOWE MATERIAŁY

Wideo - bezpieczna praca zdalna w 59 sekund

https://securityinside.com/free/video/bezpieczna_praca_zdalna_w_59_sekund/

https://securityinside.com/free/video/remote_secure_work_in_59_seconds/

NEWSLETTER

Zwiększaj świadomość cyberbezpieczeństwa w Twojej firmie. Skutecznie.

Zapisz się by otrzymywać darmowe materiały z zakresu Security Awareness. Plakaty, webinary, grafiki, filmy - po polsku.

https://mailchi.mp/d7f4da750141/securityawareness

SecurityInside

LOGICALTRUST

NASZE USŁUGI

- TESTY BEZPIECZEŃSTWA
- E-LEARNING
- TREŚCI, RAPORTY, PLAKATY
- SZKOLENIA NA ŻYWO I ONLINE
- TESTY SOCJOTECHNICZNE

ZAUFALI NAM

orange, pepsi, STATOIL, Multikino, GlaxoSmithKline, Hewlett Packard Enterprise, Santander Consumer Bank, Alior Bank, RBS, AEGON, Crédit Agricole, Getin Noble, Viessmann, money.pl, Energa, PKP Informatyka, Ministerstwo Finansów, PWPW

ZAPRASZAMY DO KONTAKTU

OFFICE@SECURITYINSIDE.COM
HTTPS://SECURITYINSIDE.COM
+48 71 738 24 35